On p-adic density of rational points on K3 surfaces

René Pannekoek

January 31, 2013

Abstract

We show that, for every prime number p, there exist infinitely many K3 surfaces over $\mathbf{Q}$ whose rational points lie dense in the space of its p-adic points. We also show that there exists a K3 surface over $\mathbf{Q}$ whose rational points lie dense in the space of its p-adic points for all prime numbers p with $p \equiv 3 \pmod 4$ and $p > 7$.

1 Introduction

In an unpublished preprint [3], Sir Peter Swinnerton-Dyer gave three non-singular diagonal quartic surfaces over $\mathbf{Q}$ together with a proof that their rational points lie dense in the space of 2-adic points. To the author's best knowledge, this is the first instance of a proof of p-adic density of rational points on any K3 surface over $\mathbf{Q}$, for any prime number p. The goal of this article is to extend the results of Swinnerton-Dyer to all prime numbers p, giving for each p an infinite number of K3 surfaces over $\mathbf{Q}$ on which the rational points form a p-adically dense set.

The K3 surfaces for which we will obtain p-adic density results will be Kummer surfaces. For an abelian variety A over a field of characteristic different from 2, let $\mathrm{Km}(A)$ denote the Kummer variety of A. It is the blow-up of the quotient $A/\langle -1 \rangle$ in the image of the 2-torsion of A. When A is an abelian variety of dimension 2, the surface $\mathrm{Km}(A)$ is a K3 surface.

We will establish the following results.

Theorem 1.1. *Let p be a prime number. Then there exist infinitely many elliptic curves E over $\mathbf{Q}$ such that the rational points of $\mathrm{Km}(E \times E)$ lie dense in the space of p-adic points.*

Theorem 1.2. *There exists an elliptic curve E over $\mathbf{Q}$ such that the rational points of $\mathrm{Km}(E \times E)$ lie dense in the space of p-adic points for all prime numbers p with $p \equiv 3 \pmod 4$ and $p > 7$.*

The proofs of Theorems 1.1 and 1.2 are given at the end of Section 3.

We end this section by fixing some notation. If E is an elliptic curve over any field k, and $c \in k^*$, then by E^c we denote the quadratic twist of E by c. If E is given by a Weierstrass equation of the form $y^2 = f(x)$, then E^c is isomorphic to the elliptic curve given by $cy^2 = f(x)$. By E_0 we denote the complement of $E[2]$ in E.

2 Elliptic curves with suitable twists

Definition 2.1. We will say that an elliptic curve E over $\mathbf{Q}$ has *suitable twists* with respect to a prime number p if for all $d \in \mathbf{Q}_p^*$ there exists $c \in \mathbf{Q}^*$ such that $d/c \in \mathbf{Q}_p^{*2}$ and $E^c(\mathbf{Q})$ is dense in $E^c(\mathbf{Q}_p)$.

Theorem 3.1 will show: if the elliptic curve E over $\mathbf{Q}$ has suitable twists with respect to p, and we have $X = \mathrm{Km}(E \times E)$, then $X(\mathbf{Q})$ is dense in $X(\mathbf{Q}_p)$.

Remark 2.2. The condition $d/c \in \mathbf{Q}_p^{*2}$ appearing in Definition 2.1 is equivalent to the twists E^c and E^d, considered as elliptic curves over $\mathbf{Q}_p$, being isomorphic over $\mathbf{Q}_p$. We may thus rephrase the fact of E having suitable twists with respect to p as follows: for all twists E^d of E over $\mathbf{Q}_p$, there exists a twist E^c of E over $\mathbf{Q}$ which is isomorphic to E^d over $\mathbf{Q}_p$, for which $E^c(\mathbf{Q})$ is dense in $E^c(\mathbf{Q}_p)$.

The remainder of this section is used to show that there exist many suitable elliptic curves E for any prime number p (Proposition 2.6).

Lemma 2.3. *Let $p > 7$ be a prime number. Let E be an elliptic curve over $\mathbf{Q}_p$ with additive reduction, and write $E^{(0)}(\mathbf{Q}_p)$ for the subgroup of $E(\mathbf{Q}_p)$ consisting of the points that have good reduction. Then $E^{(0)}(\mathbf{Q}_p)$ is topologically isomorphic to $\mathbf{Z}_p$.*

Proof. This result was already observed by Swinnerton-Dyer as Lemma 1 of [3]. The result appears with proof as Theorem 1 of [1]. For the convenience of the reader, we here reproduce the arguments from [1].

From the theory of elliptic curves over local fields (see Chapter 7 of [2]), we get an exact sequence:

$$0 \to E^{(1)}(\mathbf{Q}_p) \to E^{(0)}(\mathbf{Q}_p) \to \widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p) \to 0, \tag{1}$$

where $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)$ denotes the group of non-singular points over $\mathbf{F}_p$ on a minimal Weierstrass model of E, the arrow $E^{(0)}(\mathbf{Q}_p) \to \widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)$ is the reduction map, and we write $E^{(1)}(\mathbf{Q}_p)$ for the kernel of the reduction map. It follows from [2, IV.6.4(b)] that $E^{(1)}(\mathbf{Q}_p)$ is canonically isomorphic to $\mathbf{Z}_p$. Since E has additive reduction at p, we have $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p) \cong \mathbf{Z}/p\mathbf{Z}$. Hence, the short exact sequence (2) reads

$$0 \to \mathbf{Z}_p \to E^{(0)}(\mathbf{Q}_p) \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

It follows that the topological group $E^{(0)}(\mathbf{Q}_p)$ is isomorphic to $\mathbf{Z}_p \times \mathbf{Z}/p\mathbf{Z}$ if and only if it has non-trivial p-torsion; otherwise, it is isomorphic to $\mathbf{Z}_p$.

We will show that $E^{(0)}(\mathbf{Q}_p)$ has no non-trivial p-torsion. We will make use of a ramified field extension of $\mathbf{Q}_p$. Assume that E is given by a Weierstrass equation $y^2 = x^3 + ax + b$ that is minimal at p. Let $K = \mathbf{Q}_p(\pi)$, with $\pi^6 = p$. We define a new curve E' given by $y^2 = x^3 + a/\pi^4 x + b/\pi^6$. There is an isomorphism $\phi : E \xrightarrow{\sim} E'$ defined over K, given by $\phi(x, y) = (x/\pi^2, y/\pi^3)$. Now ϕ injects $E^{(0)}(\mathbf{Q}_p)$ into the kernel of reduction $(E')^{(1)}(K)$ of E', which by [2, IV.6.4(b)] is isomorphic to the ring of integers of K (this uses $p > 7$), which is torsion-free. So $E^{(0)}(\mathbf{Q}_p)$ is torsion-free, hence topologically isomorphic to $\mathbf{Z}_p$. $\square$

We recall that a topological group G is called procyclic if, for some $g \in G$, the subgroup generated by g is dense in G. This element g is called a topological generator of G.

Lemma 2.4. *Let p be a prime. There exist infinitely many elliptic curves E over $\mathbf{Q}$ such that, for all $d \in \mathbf{Q}_p^*$, the topological group $E^d(\mathbf{Q}_p)$ is procyclic.*

Proof. First assume $p > 7$. Choose the elliptic curve E over $\mathbf{Q}$ such that its Kodaira reduction type at p is in the set $\mathcal{K} = \{\text{II,III,IV,II}^*\text{,III}^*, \text{IV}^*\}$. It is obvious that there are infinitely many such E for each p (e.g., see the table in [2, C.15]). We will show that E satisfies the conclusion of the lemma. Note that E has additive reduction at p. The class of elliptic curves over $\mathbf{Q}$ with reduction type at p contained in the set $\mathcal{K}$ is stable under taking quadratic twists. Therefore, we may reduce to showing that $E(\mathbf{Q}_p)$ is procyclic.

From [2, C.15] we have that $E(\mathbf{Q}_p)$ fits inside a short exact sequence:

$$0 \to E^{(0)}(\mathbf{Q}_p) \to E(\mathbf{Q}_p) \to \mathbf{Z}/m\mathbf{Z} \to 0, \tag{2}$$

where $m \in \{1, 2, 3\}$. By Lemma 2.3, the topological group $E^{(0)}(\mathbf{Q}_p)$ is isomorphic to $\mathbf{Z}_p$. Since $p \nmid m$ by assumption on p, it follows that (2) splits, and that $E(\mathbf{Q}_p)$ is topologically isomorphic to $\mathbf{Z}_p \times \mathbf{Z}/m\mathbf{Z}$. This proves the lemma for $p > 7$.

For $p \leq 7$, we give examples. Let E be an elliptic curve over $\mathbf{Q}_p$ given by $y^2 = x^3 + ax + b$. Then $E(\mathbf{Q}_p)$ is procyclic in each of the cases (i) $p = 2$, $v_2(a) \geq 1$, $v_2(b) = 1$; (ii) $p = 3$, $v_3(a) = 1$, $v_3(b) > 1$; (iii) $p = 5$, $v_5(a) \geq 1$, $v_5(b) = 1$, $a \not\equiv \pm 10 \pmod{25}$; (iv) $p = 7$, $v_7(a) \geq 1$, $v_7(b) = 1$, $b \not\equiv \pm 14 \pmod{49}$. One simply shows this by looking at the various division polynomials associated to E, ruling out any unwanted torsion. This completes the proof for $p \leq 7$. ☐

We will now show that the property isolated in the preceding lemma leads to elliptic curves with suitable twists.

Lemma 2.5. *Let p be a prime, and suppose that E is an elliptic curve over $\mathbf{Q}$ such that, for all $d \in \mathbf{Q}_p^*$, the topological group $E^d(\mathbf{Q}_p)$ is procyclic. Then E has suitable twists with respect to p.*

Proof. Obviously, it suffices to assume $d = 1$, and to show that there exists a twist E^c of E with $c \in \mathbf{Q} \cap \mathbf{Q}_p^{*2}$ such that $E^c(\mathbf{Q})$ is dense in $E^c(\mathbf{Q}_p)$.

Assume that E is given by a Weierstrass curve $y^2 = f(x)$ in $\mathbf{P}^2_{\mathbf{Q}}$. Let (z, w) be a topological generator of $E(\mathbf{Q}_p)$. Let $(u, v) \in \mathbf{A}^2(\mathbf{Q}) \subset \mathbf{P}^2(\mathbf{Q})$ be chosen sufficiently close to (z, w), and such that both $f(u)$ and v non-zero. Define $c = f(u)/v^2$. Since c is arbitrarily close to $f(z)/w^2 = 1$, it is a p-adic square. Also, (u, v) lies on the curve $cy^2 = f(x)$, which we may identify with E^c. We claim that the multiples of (u, v) lie dense in $E^c(\mathbf{Q})$. Proof of claim: let $\alpha \in \mathbf{Q}_p^*$ be such that $\alpha^2 = c$. Note that α gets arbitrarily close to -1 or 1. There is an isomorphism defined over $\mathbf{Q}_p$ given by:

$$\begin{aligned} \psi : E^c &\to E \\ (x, y) &\mapsto (x, \alpha y) \end{aligned}$$

Since (u,v) was arbitrarily close to (z,w), its image $(u,\alpha v)$ is arbitrarily close to $(z,\pm w)$, and both of these points are topological generators of $E(\mathbf{Q}_p)$. Since ψ is a homeomorphism on $\mathbf{Q}_p$-points, (u,v) is itself a topological generator of $E^c(\mathbf{Q}_p)$. $\square$

Proposition 2.6. *For any prime number p, there exist infinitely many elliptic curves E over $\mathbf{Q}$ that have suitable twists with respect to p.*

Proof. This follows from Lemma 2.4 and Lemma 2.5. $\square$

3 Proofs of Theorems 1.1 and 1.2

At the end of this section we give the proofs of Theorems 1.1 and 1.2.

Theorem 3.1. *Let p be a prime number and let E be an elliptic curve over $\mathbf{Q}$ that has suitable twists with respect to p. Let $X = \mathrm{Km}(E \times E)$. Then $X(\mathbf{Q})$ is dense in $X(\mathbf{Q}_p)$.*

Proof. Recall that by E_0 we denote the complement of $E[2]$ in E. The inversion -1 on E restricts to an involution of E_0, which we will also denote by -1. The quotient $(E_0 \times E_0)/\langle -1 \rangle$, where -1 acts diagonally, is a smooth subvariety Y of X. Since no open neighborhood in $X(\mathbf{Q}_p)$ of a point in $X - Y$ can be contained in $X - Y$, it is enough to show that $Y(\mathbf{Q})$ is dense in $Y(\mathbf{Q}_p)$. Observe that Y may be identified with the open subset of
$$z^2 = f(x)f(y),$$
where z is not equal to 0.

Let $P = (\xi, \eta, \zeta)$ be a point of $Y(\mathbf{Q}_p)$. Let $d = f(\xi)$. By Definition 2.1, there exists $c \in \mathbf{Q}^*$ such that $d/c \in \mathbf{Q}_p^*$ and $E^c(\mathbf{Q})$ is dense in $E^c(\mathbf{Q}_p)$. We have a morphism:
$$q_c : E_0^c \times E_0^c \to Y$$
$$(x_1, y_1), (x_2, y_2) \mapsto (x_1, x_2, c y_1 y_2)$$
Furthermore, the point P is the image under q_c of the point $Q = ((\xi, 1), (\eta, \zeta/f(\xi))) \in (E_0^c \times E_0^c)(\mathbf{Q}_p)$. Since $E^c(\mathbf{Q})$ is dense in $E^c(\mathbf{Q}_p)$, there exists a rational point $Q' \in (E_0^c \times E_0^c)(\mathbf{Q})$ such that Q' is as close as we desire to Q, and hence such that $P' = q_c(Q') \in Y(\mathbf{Q})$ is as close as we desire to P. $\square$

Remark 3.2. What underlies our proof of Theorem 3.1 is the fact that
$$Y(\mathbf{Q}) = \coprod_c q_c((E_0^c \times E_0^c)(\mathbf{Q})),$$
where the q_c are as in the proof of Theorem 3.1, and where the c are taken over a set of coset representatives of $\mathbf{Q}^*/\mathbf{Q}^{*2}$ in $\mathbf{Q}^*$. The proof of Theorem 3.1 relies on the existence, for any $P \in Y(\mathbf{Q}_p)$, of $c \in \mathbf{Q}^*$ such that (i) P is in the image under q_c of a p-adic point on $E_0^c \times E_0^c$, and (ii) the rational points on $E_0^c \times E_0^c$ lie p-adically dense. The existence of such a c is precisely the condition that E be suitable with respect to p.

Theorem 3.3. *Let $E/\mathbf{Q}$ be the elliptic curve $y^2 = x^3 + x$ and let $X = \mathrm{Km}(E \times E)$. Then $X(\mathbf{Q})$ is dense in $X(\mathbf{Q}_p)$ for all p with $p \equiv 3 \pmod 4$ and $p > 7$.*

Proof. Let p be a prime congruent to 3 mod 4. For $d \in \mathbf{Q}_p^*$, the twist E^d of E is given by the equation $y^2 = x^3 + d^2x$. By Lemma 2.5 and Theorem 3.1, it suffices to show that $E^d(\mathbf{Q}_p)$ is procyclic for all $d \in \mathbf{Q}_p^*$. By changing to a $\mathbf{Q}_p$-isomorphic curve if necessary, it suffices to restrict to the case of $d \in \mathbf{Q}_p^*$ with $v_p(d)$ equal to 0 or 1.

First assume $v_p(d) = 0$. Let $\widetilde{E}$ be the reduction of E^d modulo p. Then $\#\widetilde{E}(\mathbf{F}_p) = p + 1$. For $p > 3$ this follows from the fact that $\widetilde{E}$ is supersingular [2, V.4.5]; for $p = 3$, one verifies it by a computation. We claim that $\widetilde{E}(\mathbf{F}_p)$ is cyclic. Suppose that $(\mathbf{Z}/\ell\mathbf{Z})^2 \subset \widetilde{E}(\mathbf{F}_p)$ for some prime ℓ. Then p must split completely in $\mathbf{Q}(\zeta_\ell)$, giving $\ell \mid p - 1$. On the other hand ℓ must certainly divide $\#\widetilde{E}(\mathbf{F}_p) = p + 1$: therefore we must have $\ell = 2$. But since $x^3 + d^2x$ splits into a linear and a quadratic irreducible polynomial over $\mathbf{F}_p$, we must have $\#\widetilde{E}(\mathbf{F}_p)[2] = 2$. This gives a contradiction, proving the claim.

By [2, VII.2.1] and the fact that E^d has good reduction at p, we have a short exact sequence:

$$0 \to (E^d)^{(1)}(\mathbf{Q}_p) \to E^d(\mathbf{Q}_p) \to \widetilde{E}(\mathbf{F}_p) \to 0,$$

where the kernel of reduction $(E^d)^{(1)}(\mathbf{Q}_p)$ of E^d is isomorphic to $\mathbf{Z}_p$ by [2, IV.6.4(b)]. We conclude that $E^d(\mathbf{Q}_p)$ is topologically isomorphic to the direct product of $\mathbf{Z}_p$ and a cyclic group of order $p + 1$. Hence $E^d(\mathbf{Q}_p)$ is procyclic.

Now assume $v_p(d) = 1$. Then E^d has additive reduction with Kodaira type IV [2, C.15], hence we have a short exact sequence

$$0 \to (E^d)^{(0)}(\mathbf{Q}_p) \to E^d(\mathbf{Q}_p) \to G \to 0,$$

where $(E^d)^{(0)}(\mathbf{Q}_p)$ is topologically isomorphic to $\mathbf{Z}_p$ by Lemma 2.3, and G is cyclic of order 1 or 3 (see [2, C.15]). Again, $E^d(\mathbf{Q}_p)$ is topologically isomorphic to the direct product of $\mathbf{Z}_p$ and a cyclic group of order 1 or 3. Hence $E^d(\mathbf{Q}_p)$ is procyclic. $\square$

Proof of Theorems 1.1 and 1.2. Theorem 1.1 follows from Proposition 2.6 and Theorem 3.1. Theorem 1.2 follows from Theorem 3.3.

4 Acknowledgements

It is a pleasure to thank Sir Peter Swinnerton-Dyer, Alexei Skorobogatov, Ronald van Luijk, Peter Stevenhagen and Jaap Top for useful discussions and encouragement.

References

[1] René Pannekoek. On p-torsion of p-adic elliptic curves with additive reduction, 2012. Preprint. See: http://arxiv.org/abs/1211.5833.

[2] J. Silverman. *The Arithmetic of Elliptic Curves, Second Edition.* Springer-Verlag, New York, 2009.

[3] H.P.F. Swinnerton-Dyer. Density of rational points on certain surfaces. Unpublished, 2010.